

Forum:[Hack Forums](#)

Thread: [Programming custom/undetectable payloads/backdoors](#)

MasterLin87 - July 3, 2019, 4:54 pm

Metasploit is a great tool, however the payloads it offers are easily detected by almost all anti-viruses and defenders out there. Even after using many layers of msfvenom encoding and using custom templates, they still kinda fail to trick the system. I am not fluent, but at least decent in python and c++. How would anyone go about programming good payloads? Are there any guides teaching how to use programming languages offensively? And how to make persistent backdoors that ask for a password permission (metasploit "run persistence" command doesn't allow you as far as I am aware).

Faith Connors - July 3, 2019, 7:25 pm

that depends on what your payload needs to do, or what you want it to do. can't just say 'how do i code a solution to lambert's problem,' because you need to understand the problem before you start working on a solution.

as far as a password goes, opt for something better: encrypting all comms to/from the shell or whatever you manage to pop. your 'password' is the encryption key and if the server receives something that cannot be decrypted with that key, then it will simply ignore it.

idk just use your head and be creative.